Notice of Allowability	Application No.	Applicant(s)	
	09/696,141	DENT, PAUL W.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment received on 9/20/2004*.

2. ☒ The allowed claim(s) is/are *1,4-18,20-27 and 31-33*.

3. ☒ The drawings filed on *25 October 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to applicant's amendment received on 9/20/04. The specification has been amended. Claims 1, 5, 12, 18 and 23 have been amended. Claims 2-3, 19, 28-30 and 34-49 have been cancelled.

Allowable Subject Matter

1. Claims 1, 4-18, 20-27 and 31-33 are allowed. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method for encrypting and decrypting messages. In particular, independent claim 1 identifies the uniquely distinct feature of adding a redundant bit to the message at a most significant bit position, modifying said redundant bit if the value of the message including the redundant bit is equal or greater than a predetermined value prior to encryption. Independent claim 18 identifies the uniquely distinct feature of appending one or more redundant bits to an information sequence to form a message having a length equal to a first modulus. Schneier discloses an encryption method comprising comparing a numerical value of a data block to a predetermined value and, if the numerical value of the data block is equal to or greater than the predetermined value, decreasing the size of the data block. Yanovsky teaches adding redundant bits to a data block to be transmitted. However, Schneier and Yanovsky fail to disclose adding a redundant bit to the message at a most significant bit position, modifying said redundant bit or

appending one or more redundant bits to an information sequence to form a message having a length equal to a first modulus.

Independent claim 23 identifies the uniquely distinct feature of adding a value equal to a modulus associated with an encryption key used to generate the doubly encrypted message. Independent claim 31 identifies the uniquely distinct feature of modifying the once encrypted bit string by adding an integer multiple of a modulus associated with an encryption key used to generate the doubly encrypted bit string to the once encrypted bit string to obtain a modified once encrypted bit string. Schneier discloses a method for decrypting a doubly encrypted message. Yanovsky teaches using redundant bits for error correction/detection. However, Schneier and Yanovsky fail to disclose adding a value equal to a modulus associated with an encryption key used to generate the doubly encrypted message or modifying the once encrypted bit string by adding an integer multiple of a modulus associated with an encryption key used to generate the doubly encrypted bit string to the once encrypted bit string to obtain a modified once encrypted bit string.

The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
2/4/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100